



# FortiClient (macOS) - Release Notes

Version 6.0.1

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



August 10, 2018

FortiClient (macOS) 6.0.1 Release Notes

04-601-498631-20180810

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Licensing	5
Standalone mode	5
Managed mode	5
<b>Special Notices</b>	<b>7</b>
Using Web Filter and Real Time Protection with FortiClient (macOS)	7
<b>What's New in FortiClient (macOS) 6.0.1</b>	<b>8</b>
New FortiClient GUI	8
Installed Software Inventory	8
Customize system quarantine message	8
Host Check and AMD support	8
Web Filter behavior when FortiGuard unavailable	8
<b>Installation Information</b>	<b>9</b>
Firmware images and tools	9
Installation options	9
Upgrading from previous FortiClient versions	9
Downgrading to previous versions	10
Uninstalling FortiClient	10
Firmware image checksums	10
<b>Product Integration and Support</b>	<b>11</b>
FortiClient 6.0.1 support	11
Language support	12
<b>Resolved Issues</b>	<b>13</b>
Malware Protection	13
Web Filter	13
Remote Access	13
Install and upgrade	14
GUI	14
Other	14
<b>Known Issues</b>	<b>15</b>
Application Firewall	15
Web Filter	15
Remote Access	15
Install and upgrade	15
GUI	16
Other	16

# Change Log

Date	Change Description
2018-08-03	Initial release.
2018-08-08	Updated <a href="#">What's New in FortiClient (macOS) 6.0.1</a> on page 8. Added <a href="#">Special Notices</a> on page 7.
2018-08-09	Updated <a href="#">Special Notices</a> on page 7.
2018-08-10	Updated <a href="#">What's New in FortiClient (macOS) 6.0.1</a> on page 8.

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.0.1 build 0028.

This document includes the following sections:

- [Special Notices](#)
- [What's New in FortiClient \(macOS\) 6.0.1](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

Review all sections prior to installing FortiClient. For more information, see the *FortiClient Administration Guide* in the [Fortinet Document Library](#).

## Licensing

FortiClient offers two licensing modes:

- Standalone mode
- Managed mode

### Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.



Support for FortiClient in standalone mode is provided on the Fortinet Forums ([forum.fortinet.com](https://forum.fortinet.com)). Phone support is not provided.

---

### Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.



When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums ([forum.fortinet.com](https://forum.fortinet.com)). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

---

## FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

## FortiClient licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

# Special Notices

## Using Web Filter and Real Time Protection with FortiClient (macOS)

When using FortiClient (macOS), Web Filter and Real Time Protection may not function properly unless the following steps are taken:

1. Reboot the Mac in recovery mode by holding down the Command and R keys.
2. Go to Utilities and start the Terminal.
3. Issue the following command:  
`spctl kext-consent disable`
4. Reboot the machine.
5. In the Terminal, enter the following command.

```
kextstat
```

The FortiClient module `com.fortinet.fct.kext.avkern2/fctapnke` should be listed. The Web Filter and Real Time Protection features should function as configured.

For the source of this solution, see [Apple Support](#).

If using MDM with an Enterprise solution, note the FortiClient team ID is AH4XFXJ7DK.

# What's New in FortiClient (macOS) 6.0.1

This section identifies the new features and enhancements in FortiClient (macOS) 6.0.1. For more information, see the *FortiClient Administration Guide*.

## New FortiClient GUI

FortiClient (macOS) 6.0.1 introduces a new UI that improves user experience and provides a refreshed look and feel. The new navigation bar provides up-to-date status information for all features while also making them more accessible.

## Installed Software Inventory

FortiClient now sends all installed software application information to EMS so it displays under *Software Inventory*. This feature requires EMS 6.0.0 or later.

## Customize system quarantine message

FortiClient can now display a customized quarantine message. This feature requires EMS 6.0.0 or later.

## Host Check and AMD support

SSL VPN now supports expanded Host Check features including verification of MAC address, running application, OS version, and file checks.

## Web Filter behavior when FortiGuard unavailable

By default, FortiClient now blocks all web traffic when FortiGuard is unreachable. You can also configure FortiClient to allow web traffic when FortiGuard is unreachable using XML configuration.



# Installation Information

## Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClient_6.0.x.xxx_macosx.dmg	Standard installer for macOS.
FortiClientTools_6.0.x.xxx_macosx.tar	Includes utility tools and files to help with installation.

The following tools and files are available in the FortiClientTools .tar file:

File	Description
OnlineInstaller	Downloads and installs the latest FortiClient file from the public FDS.



Review the following sections prior to installing FortiClient version 6.0.1: [Introduction on page 5](#), and [Product Integration and Support on page 11](#).

## Installation options

When installing FortiClient version 6.0.1, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Additional Security Features: Select one or more of the following to install: AntiVirus, Web Filtering, Single Sign On, Application Firewall

## Upgrading from previous FortiClient versions

FortiClient version 6.0.1 supports upgrading from FortiClient versions 5.2 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

## Downgrading to previous versions

Downgrading FortiClient version 6.0.1 to previous FortiClient versions is not supported.

## Uninstalling FortiClient

To uninstall FortiClient version 6.0.1, use the *Application > FortiClient > Uninstaller* application.

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at <https://support.fortinet.com>. After logging in, click on *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

# Product Integration and Support

## FortiClient 6.0.1 support

The following table lists FortiClient (macOS) 6.0.1 product integration and support information.

<b>Desktop Operating Systems</b>	<ul style="list-style-type: none"><li>• OS X 10.11 El Capitan</li><li>• macOS 10.12 Sierra</li><li>• macOS 10.13 High Sierra</li></ul>
<b>Minimum System Requirements</b>	<ul style="list-style-type: none"><li>• Intel processor</li><li>• 256MB of RAM</li><li>• 20MB of hard disk drive (HDD) space</li><li>• TCP/IP communication protocol</li><li>• Ethernet NIC for network connections</li><li>• Wireless adapter for wireless network connections</li><li>• Adobe Acrobat Reader for FortiClient documentation</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 6.0.0 and later</li><li>• 5.6.0 and later</li></ul>
<b>FortiAuthenticator</b>	<ul style="list-style-type: none"><li>• 4.2.1</li></ul> <p>FortiToken Mobile push notification is not supported for the following versions:</p> <ul style="list-style-type: none"><li>• 4.2.0</li><li>• 4.1.0 and later</li><li>• 3.3.0 and later</li><li>• 3.2.0 and later</li><li>• 3.1.0 and later</li><li>• 3.0.0 and later</li></ul>
<b>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 1.2.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 6.0.0 and later</li><li>• 5.6.0 and later</li></ul>
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• 6.0.0 and later</li><li>• 5.6.0 and later</li></ul> <p>Only IPsec VPN and SSL VPN are supported with the following FortiOS versions:</p> <ul style="list-style-type: none"><li>• 5.4.1 and later</li></ul>

## Language support

The following table lists FortiClient language support information.

Language	GUI	XML Configuration	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓		
Chinese (Traditional)	✓		
French (France)	✓		
German	✓		
Japanese	✓		
Korean	✓		
Portuguese (Brazil)	✓		
Russian	✓		
Spanish (Spain)	✓		

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.



If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

# Resolved Issues

The following issues have been fixed in FortiClient (macOS) 6.0.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Malware Protection

Bug ID	Description
476454	Exclusions not being obeyed on FortiClient (macOS).
492038	<code>&lt;block_removable_media&gt;0&lt;/block_removable_media&gt;</code> where is it in EMS 6.0 and Windows FortiClient 6.0?

## Web Filter

Bug ID	Description
445380	Add option to show block message from FortiClient bubble popup for HTTPS site.
462107	AFP access is slow when Web Filter or malicious websites is enabled.
465234	Captive portal app shows blank page.
469400	Misspelled XML attribute in FortiClient (macOS) 5.6.3.
477771	Add option to not block "unrated" if FortiGuard cannot be contacted.
485005	Support new Web Filter categories (9X) in FortiClient and EMS.

## Remote Access

Bug ID	Description
459788	Memory leak in SSL VPN.
458782	Unable to connect to IPsec VPN using okta two factor authentication.
467414	SSL VPN issues using FortiClient (macOS).
482160	SSL VPN split tunneling does not work for DNS resolution - SSL custom DNS replaced system DNS.

## Install and upgrade

Bug ID	Description
475421	FortiClient (macOS) update does not try to contact more than one server.
473975	FortiClient managed by corporate EMS on Mac removes custom VPN profiles upon upgrade.
471128	SSO-only installer for Mac.
487211	FortiClient would not automatically start on other users on macOS 10.13 High Sierra.

## GUI

Bug ID	Description
503405	Vulnerable application path does not show vulnerable file.

## Other

Bug ID	Description
477322	Update AV and IPS engines and signatures to new versions.
491488	Should update IPS engine when Application Firewall is not installed.
502108	FSSO agent does not communicate to FortiAuthenticator.

# Known Issues

The following issues have been identified in FortiClient (macOS) 6.0.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Application Firewall

Bug ID	Description
494032	Selecting <i>Block known attack communication channels</i> fails.

## Web Filter

Bug ID	Description
498203	Exclusion list does not block pages.

## Remote Access

Bug ID	Description
505349	<i>Save Password</i> , <i>Auto-connect</i> , <i>Always up</i> do not work properly.

## Install and upgrade

Bug ID	Description
495862	IPsec pre-shared key lost when package installed by another user on the same endpoint.

## GUI

Bug ID	Description
467328	Logs for vulnerability scan should include file path.

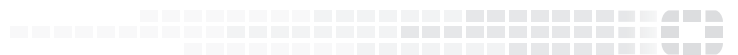
## Other

Bug ID	Description
479913	Quarantined Mac PC does not block traffic.





**FORTINET®**



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.